FRANCE PAYMENTS FORUM

Rencontre digitale du 25 septembre 2025

Intervention d'Éric Ducoulombier (Commission européenne)

Le point sur les projets réglementaires en cours

Les projets de règlement et de directive sur les services de paiement (DSP/RSP)

Planning des négociations

Concernant les travaux sur la révision de la DSP et sur le RSP, comme l'a indiqué Hervé Sitruk, nous en sommes au stade des trilogues. Nous avons eu un premier trilogue en juillet, un deuxième avant-hier (23 septembre) et nous en aurons un troisième le 23 octobre. L'atmosphère est bonne. Du côté du Parlement comme du Conseil et de la Commission, tous sont assez impatients de finaliser les travaux. Mais cela ne veut pas dire qu'un accord sera atteint à n'importe quel prix. Les trois parties prenantes du trilogue ont chacune leurs positions, qui sont maintenant connues puisqu'elles ont été publiées

La présidence Danoise effectue un travail remarquable pour la préparation de ces trilogues. Ils s'investissent énormément et y consacrent beaucoup de ressources. J'espère qu'ils seront récompensés par un accord politique à Noël.

Principaux sujets en discussion

La plupart des sujets traités dans cette phase de trilogue sont considérés comme techniques et examinés en trilogue technique. Mais le sujet principal examiné en trilogue politique est la fraude. J'ai le sentiment que si nous trouvons un compromis sur la fraude, les sujets « techniques » (open banking, transparence des frais, e-money…) suivront.

Trilogue politique : la lutte contre la fraude

Deux points sont, depuis le début, au cœur des discussions (a) la notion d'autorisation ; (b) la responsabilisation des acteurs non financier de la chaîne des paiements (telcos),

La notion d'autorisation

Tout le monde est conscient que depuis la DSP2 (donc depuis 2015), la notion d'autorisation ou de non-autorisation doit évoluer, parce que la fraude telle qu'elle existait il y a 10 ou 15 ans a été largement supplantée par de nouveaux types de fraudes basés sur la manipulation du payeur, souvent avec des techniques d'hameçonnage, etc.

Donc, tout le monde est conscient qu'une grande partie des transactions qui sont techniquement autorisées, mais qui, en réalité, ont été autorisées dans des circonstances où la volonté de la victime a été manipulée, constituent de nouvelles formes de fraudes qui

appellent de nouvelles règles juridiques. Mais il s'avère compliqué de s'entendre sur une définition commune.

- Le Conseil est plutôt sur une approche objective : il y a autorisation si des critères objectifs sont remplis.
- Le Parlement est plutôt sur une approche subjective : quelle était l'intention réelle du consommateur ? Avait-il l'intention d'effectuer une telle transaction ? S'il avait su qu'elle était frauduleuse, l'aurait-il faite ?

Le rôle de la Commission est d'être un « pont » entre les deux co-législateurs, pour tenter de combiner ou réconcilier les deux approches. Nous sommes en train d'y travailler, c'est tout l'enjeu des discussions en trilogue.

La responsabilisation des « telcos »

Aujourd'hui, la chaîne des paiements s'est beaucoup complexifiée, et la chaîne de la fraude s'est elle aussi complexifiée. Une grande majorité des fraudes au paiement trouvent leur origine dans des arnaques nées sur Internet ou via un SMS ou un appel téléphonique.

Quel doit être le rôle des fournisseurs de services de communication électronique (opérateurs télécom, plateformes, réseaux sociaux… en bref les « telcos ») dans la prévention de la fraude et, le cas échéant, dans la responsabilité pécuniaire d'indemnisation d'un victime ? Ici aussi, les deux co-législateurs ont des positions assez différentes :

- Le Conseil a une approche plutôt conservatrice.
- Le Parlement a une approche plus « pro-consommateur » consistant à donner une certaine responsabilité aux telcos.

Les discussions sont rendues complexes, à la fois par la complexité du sujet, mais aussi par le fait qu'il existe des règles européennes, notamment le Digital Services Act (DSA), qui postule un principe général d'irresponsabilité des plateformes, sauf quand certaines conditions sont remplies. Mais ce postulat, c'est plutôt l'irresponsabilité des plateformes, qui ne peuvent pas discipliner tous les contenus susceptibles de transiter par leur réseau. Ce n'est que dans l'hypothèse où ces plateformes auraient été informées du caractère illégal d'un contenu qu'elles doivent le retirer : elles n'ont pas d'obligation de surveillance, à titre préventif, des milliards de données qui passent chaque seconde sur leurs plateformes.

Vous voyez donc la difficulté : ces règles européennes ont été adoptées avec d'autres objectifs que la prévention de la fraude, mais quand on les examine dans le cadre de la prévention de la fraude, elles peuvent éventuellement constituer des obstacles. Nous sommes à la manœuvre avec nos collègues de la DG Connect (qui sont les gardiens de cette réglementation), pour voir comment faire en sorte que cette réglementation puisse être considérée comme un levier plutôt que comme un obstacle. Je suis assez optimiste, car nos collègues participent de manière constructive aux discussions.

Vous avez d'ailleurs peut-être vu que la Commission a annoncé qu'elle ouvrait des enquêtes avec Apple, Microsoft, Google et Booking sur leurs politiques et leurs actions en matière de fraude au paiement. Ce calendrier n'est pas une pure coïncidence : la DG Connect a voulu montrer qu'elle était pleinement investie dans la lutte contre la fraude au paiement, et que le DSA n'est pas un obstacle, mais peut être une arme contre les fraudeurs.

Nous en sommes encore au début. Lors du trilogue du 23 septembre, les co-législateurs ont présenté leurs positions et la Commission a rappelé sa proposition, basée sur une coopération entre les différents acteurs de la chaîne des paiements. La négociation proprement dite se déroulera probablement lors du trilogue du 23 octobre, mais d'ici là un gros travail sera effectué en coulisses pour préparer les discussions et tenter de trouver des compromis, à la fois sur la notion d'autorisation et sur la responsabilisation des « telcos ».

Les trilogues techniques

En parallèle de ces trilogues politiques (qui se déroulent seulement un jour par mois), il y a beaucoup de trilogues techniques. Les experts de la Commission, du Parlement et du Conseil se rencontrent à peu près 3 fois par semaine pour progresser sur tous les autres sujets, qui sont considérés comme relevant plutôt du domaine technique.

L'euro numérique

On est encore au stade de la préparation des positions, tant au niveau du Conseil que du Parlement européen.

Au niveau du Conseil

Parmi les pierres d'achoppement, le sujet le plus sensible était le processus par lequel seraient définies les limites de détention (« *holding limits* »). Aucune solution n'ayant pu être trouvée au niveau des experts du Conseil, le sujet a dû être remonté au niveau des ministres de l'Eurogroupe.

Vendredi dernier (19 septembre) à Copenhague, l'Eurogroupe a trouvé un accord. Le processus par lequel seront définies les limites de détention implique à la fois la BCE et les États membres (qui voulaient avoir leur mot à dire et ne pas laisser entièrement le champ libre à la BCE). C'est d'ailleurs le même processus qui présidera à la décision finale d'émettre l'euro numérique. Ce processus, mis au point par les juristes de la BCE, de la Commission et du Conseil qui ont beaucoup « phosphoré » inclut des délais et une arborescence. Le contenu de cet accord sera inséré dans la proposition sur l'euro numérique.

Quelques autres sujets restent sur la table, moins « politiques » que les limites de détention mais néanmoins importants, comme par exemple la rémunération des banques pour le service de distribution de l'euro numérique qu'elles fourniront.

Au niveau du Parlement

Comme vous le savez, le rapporteur espagnol, Fernando Navarrete n'est pas un fan de l'euro numérique (il n'en fait pas mystère et l'a largement fait savoir). Il a organisé pendant l'été une série d'auditions techniques avec la Commission, la BCE et beaucoup d'acteurs des paiements. Il a annoncé il y a quelques jours son intention de présenter son projet de rapport dans les semaines qui viennent, l'objectif étant que ce rapport puisse être adopté par le Parlement européen en mai prochain.

Au sein du Parlement, il y a un clivage gauche-droite (avec aussi parfois certains clivages nationaux) : la gauche est plutôt en faveur de l'euro numérique ; la droite (le PPE, dont fait partie Fernando Navarrete) est plutôt sceptique.

Calendrier prévisionnel

Le Conseil et le Parlement pourraient se retrouver en trilogue en juin prochain pour essayer de finaliser le travail à fin 2026. Il faudra alors que la BCE s'appuie sur cette réglementation pour finaliser son propre parcours. C'est donc en 2028 ou, plus probablement, en 2029 qu'on pourrait commencer à avoir des euros numériques.

Pendant ce temps-là, comme nous l'expliquera Laetitia Dorla, le secteur privé n'a pas chômé. Vous avez tous vu l'avancement très encourageant des travaux entre EPI et EuroPA. Nous sommes très satisfaits que les différents « consortiums » qui jusque récemment travaillaient un peu chacun dans son « couloir » se soient rapprochés et développent des projets communs. C'est une excellente nouvelle.

Il faudra voir ce que cette coopération pourra donner concrètement, mais c'est à l'évidence un élément dont devront tenir compte, le moment venu, ceux qui décideront d'émettre (ou non) l'euro numérique. Quel sera, à ce moment-là, l'état de la souveraineté européenne dans le domaine des paiements et l'état d'avancement des travaux sur les produits et solutions développés par les acteurs privés ?

Tout cela devra entrer dans le débat. Mais nous n'en sommes pas encore là

La Verification of Payee (VoP)

La date du 9 octobre s'approche à grand pas. Nous parlons beaucoup avec l'EPC, avec les banques, avec les trésoriers d'entreprises, avec les consommateurs, avec les États membres, avec les superviseurs… afin de s'assurer que tout le monde est bien en ordre de marche et que le 9 octobre sera un succès. Nous n'en doutons pas, puisque les préparations ont été accomplies selon les calendriers nécessaires par tous les acteurs, mais c'est une grande migration. La VoP existait dans quelques États-membres mais était peu utilisée. Maintenant, la VoP va exister dans tous les État-membres (de la zone euro dans un premier temps) et aussi dans les transactions transfrontières. C'est donc vraiment une nouveauté.

Nous sommes conscients que tout le monde ne sera sans doute pas prêt le 9 octobre et qu'il faudra peut-être « peaufiner » dans les jours et dans les semaines qui suivront, mais grosso modo, nous avons le sentiment que le 9 octobre sera un succès. Nous sommes également conscients que la VoP n'est pas la baguette magique contre la fraude, mais c'est déjà une contribution très importante.

Merci de votre attention.

***

Questions-réponses

Cathie-Rosalie Joly

Nous avons tous conscience que la lutte contre la fraude est un point majeur des négociations en cours sur DSP/RSP. Pourriez-vous nous éclairer sur la manière dont ces nouvelles dispositions encore en discussion s'articuleront avec le principe d'irrévocabilité des paiements ?

Éric Ducoulombier

Durant les discussions, notamment sur le volet prévention de la fraude, l'idée a émergé que lorsqu'il y a un soupçon avéré de fraude, une banque pourrait bloquer une transaction, c'est-à-dire ne pas l'exécuter, contrairement à l'instruction qu'elle a reçue. Les discussions tournent autour des précautions à prendre pour éviter qu'une banque bloque des transactions sans avoir des éléments tangibles qui lui permettent de croire que c'est une transaction frauduleuse. Mais tout le monde a accepté l'idée que pour la prévention de la fraude, il peut y avoir une entorse aux principes d'irrévocabilité ou d'obligation d'exécution de la transaction par la banque.

Dans la DSP2, on faisait seulement état de la possibilité de bloquer un instrument de paiement (ex : bloquer une carte), mais la discussion s'est déplacée sur la possibilité de bloquer aussi une transaction donnée. Mais il faut s'entourer de certaines précautions pour éviter une éventuelle légèreté de la part de la banque dans la décision de bloquer des transactions. Il faut vraiment que la banque, sur la base des outils de détection dont elle dispose, ait une quasi-conviction (plus qu'un simple soupçon) qu'une transaction doit être bloquée, bien que le payeur en ait demandé l'exécution. À charge bien sûr pour la banque de vérifier rapidement si ces soupçons étaient légitimes ou pas, pour que la transaction puisse, s'il y a lieu, être rapidement débloquée.

La fraude est considérée comme un tel fléau que l'on peut faire des entorses à certains principes qui étaient considérés comme intangibles à l'époque de la DSP2 : on a changé d'époque et la fraude justifie ce genre de mesures.

On parle de bloquer une transaction, mais on parle aussi d'introduire des « *spending limits* » pour que le consommateur puisse définir des limites au montant des transactions, et qu'il puisse aussi, lorsqu'il change ses limites de transaction, avoir une période de réflexion (« *cooling off* ») de quelques heures avant l'entrée en vigueur des nouvelles limites, ceci au cas où, par exemple, il se rendrait compte qu'il a relevé ses limites en ayant été manipulé par un fraudeur.

Hervé Sitruk

Deux questions:

- *Où en est l'idée d'un équivalent européen de l'OSMP français : trouvera-t-elle des suites dans la DSP ou plus tard ?*
- *Autre sujet qui nous préoccupe : en 2027, le Règlement eIDAS2 devrait s'appliquer au paiement. Un certain nombre d'experts nous disent que ce n'est pas aussi évident que cela, même si des consortiums ont été créés et des pilotes ont été lancés. Quid du lien entre eIDAS2 et la DSP et, plus généralement, du lien entre la DSP et d'autres réglementations autour de la DSP, telles que MiCA, DORA*

Éric Ducoulombier

Equivalent européen de l'OSMP français

Aujourd'hui, effectivement, dans le texte du RSP, il y a un article qui invite la Commission à mettre sur pied une telle structure. L'idée n'est pas du tout controversée, bien au contraire : nous y sommes très favorables et les co-législateurs aussi. Cette disposition devrait donc figurer dans le texte final.

Ensuite, il faudra comment composer de manière harmonieuse cette structure (Forum, Observatoire…il faudra voir comment l'appeler. Ce sera un groupe d'experts, mais il ne faut pas que ça soit une « usine à gaz » avec des centaines de participants. Cela sera sans doute compliqué car nous devrons avoir autour de la table tous les acteurs, or il y en a de plus en plus dans le domaine des paiements. Mais nous y arriverons. De telles structures existent dans d'autres domaines, par exemple la finance durable, et nous nous inspirerons des bonnes pratiques de certains de nos collègues. Et nous nous inspirerons aussi, bien sûr, de la bonne pratique française de l'OSMP dont Julien Lasalle nous parlera tout à l'heure.

Liens entre les diverses réglementations

C'est un peu une galaxie avec différentes planètes. La DSP et le RSP sont au centre de notre galaxie, mais nous sommes conscients que beaucoup d'autres textes européens interagissent avec les paiements : l'identité numérique, MiCAR, l'euro numérique, FIDA, et encore d'autres textes qui sont soit en discussion, soit déjà en vigueur.

Nous passons beaucoup de temps à veiller à une articulation harmonieuse entre tous ces textes, notamment entre MiCAR et DSP : il y a en effet un chevauchement puisque MiCA dit

que les e-money tokens sont des fonds qui, à ce titre, tombent aussi dans le champ d'application de la DSP2 et de la future DSP3. Et l'industrie nous dit « Attention aux doubles réglementations ! Ne nous mettez pas un sac de ciment sur le dos alors que nous sommes dans un marché global très concurrentiel». Nous comprenons bien tout cela, mais nous devons jongler avec des textes qui existent : on ne peut faire dire à MiCAR ce qu'il ne dit pas.

Nous nous efforçons donc, en liaison avec l'Autorité Bancaire Européenne (ABE), d'articuler les textes existants. C'est dans cet esprit que l'ABE a publié en juin dernier une *No-action letter*[1] sur l'articulation entre la DSP et MiCAR. De même nous nous efforçons, avec les co-législateurs, de prévoir le régime futur en veillant à ce que certaines règles provenant du monde des paiements soient applicables lorsque ces instruments sont utilisés comme s'ils étaient des moyens de paiement.

Parmi ces textes, il y a bien sûr l'identité numériques (eIDAS2), dossier que nous suivons particulièrement avec nos collègues de la DG Connect. Nous savons que le marché a certaines interrogations sur l'articulation entre la future identité numérique et les règles des paiements, notamment en matière d'authentification forte. Le débat est toujours ouvert, mais nous avons apporté des réponses : nous avons organisé des workshops avec l'industrie là-dessus, et nos collègues de la DG Connect ont donné quelques réponses via une FAQ.

Cathie-Rosalie Joly

En ce moment, nous observons une avalanche de réglementations. Je dis « avalanche » par référence à la superposition et à la complexité des instruments juridiques actuels - directives, règlements, règlements techniques d'application - qui nécessitent un travail d'analyse et d'implémentation considérable.

Suivant la nature de l'instrument juridique choisi, on va avoir plus ou moins de « gold-plating » (surtransposition). Avec une directive, le niveau d'harmonisation est moindre qu'avec un règlement. Dans le cadre DSP3/RSP, on note que la partie agrément relève de la directive (DSP3) alors que la partie lutte contre la fraude relève du règlement (RSP).

Ceci soulève des questions quant aux marges de manœuvres laissées aux États dans le cadre des agréments et des implications possibles en matière de choix d'installation des nouveaux acteurs, puisqu'avec le passeport européen, dès lors qu'on est autorisé dans un pays on peut proposer ses services dans l'ensemble des États européens. Comme vous l'avez vu, l'AMF et ses homologues autrichienne (FMA) et italienne (Consob) ont il y a quelques jours appelé de leurs vœux une supervision directe au niveau européen des principaux fournisseurs de services sur crypto-actifs.[2]

[1] EBA publishes No Action letter on the interplay between Payment Services Directive (PSD2/3) and Markets in Crypto-Assets Regulation (MiCA) | European Banking Authority

[2] Les autorités de marché française, autrichienne et italienne appellent à un cadre européen renforcé des marchés de crypto-actifs | AMF

***Ma question porte donc** sur l'évolution de la coordination au niveau de la supervision entre les différents États. Comment envisagez-vous le renforcement de l'harmonisation supervisorielle pour optimiser le fonctionnement du marché unique et du passeport européen et éviter la tentation du « forum shopping réglementaire » ?*

Éric Ducoulombier

Sur votre premier point, il est vrai que nous avons réparti les choses entre une directive et un règlement :

- Les obligations qui incombent aux États et aux autorités de contrôle ont été mises dans la directive (DSP3).
- Les dispositions adressées à des acteurs du marché (banques ou Fintech) et aux consommateurs ont été mises dans le règlement (RSP). De ce fait, elles ne pourront pas faire l'objet de « gold-plating », puisqu'un règlement ne donne pas lieu à transposition.

Sur votre deuxième point, nous avons bien identifié le risque de « forum shopping ». Mais celui-ci peut être aussi dû à des considérations fiscales et pas seulement à une réglementation plus légère. Les réglementations européennes en matière de banque et de Fintech doivent s'appliquer de la même manière, et l'un des rôles de l'ABE est de parvenir à une convergence sur les pratiques et les standards de supervision.

Certes, on observe que 90% des Fintechs dans le domaine des paiements se sont fait agréer en Lituanie, en Irlande ou au Luxembourg. Mais nous n'avons pas de raisons de penser que c'est parce que la réglementation est plus légère dans ces pays. En revanche, il peut y avoir des questions de rapidité, d'efficacité. On me dit souvent qu'en Lituanie on obtient la licence de manière beaucoup plus rapide qu'ailleurs, mais personne ne m'a apporté d'éléments qui démontreraient que la réglementation est plus accommodante en Lituanie.

Il est vrai qu'en parallèle avec tout cela, notamment dans le contexte de l'Union des Marchés de Capitaux, il y a des réflexions en cours sur l'opportunité d'une supervision centralisée au niveau européen en matière de post-trading ou de cryptoactifs, avec l'idée que l'ESMA pourrait être le superviseur unique. Mais en matière de paiement, ce débat n'est pas sur la table : nous n'avons pas l'impression qu'il y ait des problèmes de « forum shopping », mais si c'était le cas, bien évidemment, nous examinerions le problème.

Dernière point que je voudrais évoquer : la simplification. Deux mots-clés dominent les discussions en ce moment : souveraineté et simplicité. Le domaine des paiements n'y échappe pas : dans les travaux DSP/RSP, nous nous demandons à tout moment si ce que nous faisons « tient la route » en termes de simplicité.

Nous ne voudrions pas que dans quelques années, nos successeurs soient contraints de faire un « omnibus » sur les paiements pour simplifier ou déréglementer ce qui aurait été harmonisé de manière trop complexe. Nous avons la chance d'être encore en discussion et d'avoir à l'esprit cette exigence de simplification : s'agissant par exemple des mandats de niveau 2 ou des guidelines de niveau 3, nous essayons de faire en sorte que le cadre juridique futur soit simple et clair.

Ce n'est pas toujours facile, car il faut parfois trouver des compromis, c'est-à-dire mettre 27 États-membres d'accord entre eux, puis avec le Parlement, le tout sans fâcher la Commission. Cela peut expliquer que certains compromis soient un peu complexes, mais la présidence danoise a fait de la simplification l'une de ses priorités.

Jacques Vanhautère

Deux points rapides à propos de la VoP :

- *Tout le monde ne sera pas prêt le 9 octobre.*
- *Au démarrage, la VoP aura un impact très fort sur les paiements, car c'est complètement nouveau pour l'ensemble des acteurs.*

Nous espérons bien sûr que le « match » sera majoritaire et que la qualité est là, mais on sait bien qu'en pratique ce n'est pas le cas. Les web-banking sont remplis de noms du genre « maman » ou « mon petit poussin » qui déclencheront des alertes (prévues dans l'IPR), avec pour effet que les particuliers arrêteront de faire des paiements. Nous allons donc avoir une courbe en « J ». L'enjeu est de savoir quelle sera la profondeur de cette courbe en « J ».

Éric Ducoulombier

Merci Jacques, j'en suis bien conscient. Désolé, mais je dois partir (je suis attendu).

Hervé Sitruk

Merci beaucoup, Éric.